

**Amendments To The Drawings**

Please amend Figure 5, by adding step 505, as shown in the accompanying revised drawing for Fig. 5, labeled "Replacement Sheet".

**REMARKS****I. Status of the Claims**

Claims 1-52 were rejected by the Examiner in the Office Action. Claims 1-52, as amended, remain in the case.

No new matter has been added by this amendment to the claims, the specification, or the drawings.

**I. Response to the Objections to the Specification:**

The Examiner has objected to various minor informalities in the specification. On page 5, line 21, the word another has been misspelled ("anoter"). On page 8, line 5, CCC 313 is mentioned, however, the Examiner suggests that reference should actually read CCC 310 per FIG. 3A. The Examiner has further indicated that there is no item "505" in FIG. 5.

In response, the Applicant has amended Figure 5 to add step 505, paraphrasing the text in the Applicant's specification at page 10, lines 10-13. Additionally, the specification has been amended to correct the word "anoter" to "another" and correct "CCC 313" to read -- CCC 310 -- in accordance with the Examiner's suggestions.

**II. Rejections Under 35 U.S.C. §102(a):**

Claims 1-9, 13-20, 22-26, 39-42, 52 have been rejected under 35 USC § 102(a) as being anticipated by US 6,282,362 B1 to Murphy (Hereafter, "Murphy"). More specifically, the Examiner contends that Murphy anticipates each and every limitation of the aforementioned claims.

Before addressing this ground for rejection, the Applicant would like to draw the Examiner's attention to some of the novel and unobvious features of the claimed invention. The Applicant's claimed invention authenticates multimedia content, such as audio, video and photographic images, by creating a combined expression comprising the content and at least the data representing the location of its creation. The claimed invention then computes a hash value on the combined expression of content and location data. The resulting hash value uniquely ties the content to the circumstances of its creation, e.g., the location and time of its creation, and also ensures the data integrity of the content, that the content has not been altered by unauthorized entities.

One aspect of the Applicant's claimed invention is described in the Applicant's specification at Page 5, lines 7-13, which reads as follows:

The system then secures the authentication data to the content through content encryption **107**, metadata encryption **108**, and/or a "hash" encryption **109**, each of which is well-known in the art. Once an encrypted signature based on the authentication data **103**, **104**, and **105** is integrated into the content file, the file is then transmitted to a Content Certification Company (CCC) **110**, or other distributor or Rights Management (RM) provider.

A further aspect of the Applicant's claimed invention is described in the Applicant's specification at Page 10, line 14 to page 11, line 2, which reads as follows:

"One example of media encoding is given in Figure 6. In this example the metadata file 601 comprises, in addition to the location signature data such as location, date, time, device and/or user identifying data and file size, also a "hash" signature of content file 600. In the example, the "hash" signature is shown as "acek321idksl", which is created by using an "hash" algorithm. The "hash" signature can be used for detecting any tampering with the content. The "hash" algorithm can be selected from a plurality of algorithms available on the mobile device. An ID for the selected algorithm can be included in the metadata of the content file. The CCC can identify the used algorithm based on the ID and can run a check for identifying any tampering on the content file. In another embodiment of the invention the "hash" algorithm can be applied to the metadata associated with the content and his "hash" is sent to the CCC. "

Turning now to the Murphy reference cited by the Examiner, Murphy discloses steganography or watermarking the content image by replacing selected pixels in the image by selected bits from a binary expression of the location and/or time of the image's creation. For example, Murphy describes watermarking the content image at Column 20, lines 37-47, which reads as follows:

"In a second embodiment of the image authenticating version of the present invention, the position information is automatically recorded or embedded as part of the corresponding digitally expressed lineage formed by the digital camera, using the bit array A shown in FIG. 6. Here, a pattern P of pixels is chosen in the digital image. For each pixel in the pattern P, one or more bits in the representation of the pixel value is replaced by a bit in the bit array BA, and the original digital image is reformed as a modified digital image, now containing the position information recorded at the time the original digital image was formed."

Murphy also discloses a first embodiment at column 20, lines 5-36, wherein a first subframe contains the image data and a second, adjacent subframe shown in Fig. 6 contains a concatenated expression containing the location data, time data, etc. as shown in Fig. 6.

Neither Murphy's first embodiment nor the second embodiment disclosed or suggests the Applicant's claimed invention of computing a hash value on the combined expression of content and location data.

The Examiner has rejected claim dependent 22, which claims "the at least one encryption algorithm is a hash algorithm," the Examiner referring to Murphy's reference at Column 22, lines 6-27. Murphy's recitation, in part, reads as follows:

"Alternatively, the encryption key can depend upon the content of the position information. In this alternative approach, a selected part, or all of, the position information is treated as one or more parameters that determine the encryption key. For example, the location information and/or angular orientation information and/or time information can be expressed in bit array format and can be combined, bit by bit, with a selected bit pattern of appropriate length L, using EXclusive Or or EXclusive NOR or twos complement addition, to form an encrypted bit array BA<sub>enc</sub>. The encrypted bit array BA<sub>sub.enc</sub> is then placed in the second sub-frame associated with the digital image in the first sub-frame (first embodiment) or is used to replace selected bits in the pixel value representation for the pixels in a pixel pattern P, such as shown in FIG. 7."

This disclosure by Murphy merely uses the location and/or time information as an encryption key to encrypt the second subframe containing the concatenated location, time, etc. shown in Fig. 6. This is not performing any computation on the image content, itself, but merely encrypting the location and time data. This is not a hash algorithm and it is not the computation of a hash value on the combined expression of content and location, as claimed by the Applicant.

There is nothing in the section of Murphy that the Examiner points to, nor is there anything elsewhere in the Murphy reference disclosing or suggesting the Applicant's claimed invention of computing a hash value on the combined expression of content and location data.

Accordingly, the Applicant respectfully requests the Examiner to withdraw this rejection of Applicant's claims over the Murphy reference.

### **III. Rejections Under 35 U.S.C. §103(a):**

Claims 10, 11, 20, 21, 37, 38, 50 and 51 have been rejected under 35 USC § 103(a) as being unpatentable over USP 6,282,362 B1 to Murphy in view of US Patent

Publication 2002/0080968 A1 to Olsson (Hereafter, "Olsson"). More specifically, the Examiner contends that the combined teachings of the Murphy and Olsson references make obvious claims 10, 11, 20, 21, 37, 38, 50 and 51.

Olsson discloses a system for providing location based service from a third party service provider, which encrypts the client's identification information to protect the client's anonymity. The Examiner has relied upon Olsson to make obvious the claimed requirements of the present invention for device identification via an IMEI and IMSI number (see for example claims 10 and 11).

The Olsson reference does not cure the deficiencies of the Murphy reference. There is no disclosure or suggestion in either the Olsson reference taken alone or in combination with the Murphy reference of the Applicant's claimed invention of computing a hash value on the combined expression of content and location data.

Accordingly, the Applicant respectfully requests the Examiner to withdraw this rejection of Applicant's claims over the combination of the Murphy reference and the Olsson reference.